The Price of Security: The Challenge of Measuring Business Value Investments in Securing Information Systems

Tony Coulson
California State University, San Bernardino
5500 University Parkway
San Bernardino, CA 92407
Phone: 909-537-5768, Email: tcoulson@csusb.edu

Jake Zhu
California State University, San Bernardino
5500 University Parkway
San Bernardino, CA 92407
Phone: 909-537-5068, Email: jzhu@csusb.edu

Shan Miyuan
Hunan University, Changsha
Hunan, P. R. China, 410082
Phone: 86 (731) 882-3903, Email: shanmiyuan@163.com

C.E. Tapie Rohm
California State University, San Bernardino
5500 University Parkway
San Bernardino, CA 92407
Phone: 909-537-5786, Email: trohm@csusb.edu

ABSTRACT

With powerful regulations surrounding security and privacy of information, the authors attempt to identify challenges valuing information security investments. The authors examine three primary approaches to measuring information value: Perceived, Real, and Normative. Literature is reviewed and the approaches are examined in terms of their strengths and weaknesses in providing value measurements for secure information systems. A framework is presented to suggest at what level in an organization and in what situations these information value approaches are most suitable.

Keywords: Security, Value, Information Systems, Perceived, Normative

INTRODUCTION

"When you can measure what you are speaking about and express it in numbers, you know something about it."
- Lord Kelvin

"Network security experts can't measure their success without metrics, and what can't be measured can't be managed."
- William Boni, CISO, Motorola Inc.

Information has become a major economic good which has added considerably to the magic of information technology/information systems (IT/IS) as well as the mystique of IT/IS. IT/IS has always been a wild card in business, a source of opportunity and uncertainty, advantage and risk. CEOs sometimes have difficulty seeing the strategic impact that IT/IS can bring to business while information managers don't understand why CEOs can't grasp the concept and seize the potential benefit created by IT/IS. Both struggle as they attempt to implement increasingly complex systems in rapid changing IT/IS environment (Applegate et al., 2003).

This has become further complicated by recent security challenges related to information systems. While an organization still needs to compete effectively in a global environment, government regulations are now required to protect information quality and privacy. Further complicating the environment is the complex web of security risks such as worms, viruses, hackers, and rogue employees that each bring about a need for tighter controls (Nicolett, 2004). Many firms have created executive positions such as the Chief Security Officer, to oversee these protection efforts and develop cost-effective solutions.

Ongoing investments in securing computing technologies are lofty for many firms. Information Managers and Security Officers find it increasingly difficult to justify their pending investments/expenses in security as many past studies have exhibited inverse impacts of the dollars spent for information technologies on the bottom line of the firm (Brynjolfsson, 1993). As technologies continue to advance so dramatically, the problems associated with measuring the bottom-line contribution of information technology is difficult. Adding security and regulatory requirements makes these problems even more severe.

HOW DO IT/IS SECURITY INVESTMENTS IMPACT A FIRM'S PERFORMANCE?

The goal of a firm is to grow, either in market share or in sales or both. In the modern organization environment, doing so requires a secure environment in which to increase capacity, productivity, while reducing costs, and hence prices. Several studies have been performed to determine the relationship between IT/IS and performance and productivity. Results are contradictory, inconclusive and usually non-generalizable (Lee & Bose, 2003). The one constant is that there is a requirement for reliable value metrics. It is already known that reliable metrics can strongly influence individual decision making and behavior and choosing the wrong metrics can lead an organization to devote its limited time and resources toward unproductive activities (Nicolett, 2004).

Often a firm's IT value measurements are performed in a variety of ways, including Return on Assets (ROA), Return on Investment (ROI), sales growth and market share. Research shows that outcomes might not be as expected. For example, a study by Mitra & Chaya (1996) found within their sample companies that IT investments were associated with lower average production costs and lower average total costs. However, the research also indicated that IT investments (which typically include security infrastructure) often contribute to higher than average overhead costs and show no evidence to support reduced overall labor costs, as is often cited as a justification for system purchases. Furthermore, Mitra & Chaya (1996) also discovered that IT infrastructure investments have zero net present value, which means they are not worth more than they cost over time due to rapid depreciation of technology and increasing support costs, including security. The firms that beat these findings and were able to better realize an increased market value all had one common element: innovative IT investments. The problem is that innovative investments are less common than the maintenance of vast IT and security operations.

While Mitra & Chaya (1996) were able to measure some increases in market value through IT alignment with business strategy, there remains a question about whether this translates into profit. Mahmood & Mann (1993) showed that a company can increase productivity from effective management of IT without experiencing higher profitability. They explain these findings by suggesting that, on average, companies make IT investments just for sustaining competitive advantage but not gaining it (Mahmood & Mann, 1993). A later study by Sircar et al. (2000) also supports the concept of IT investment not translating into profits. These authors found that IT investments had a strong positive relationship with sales, assets and equity, but not with net income. Thus, the linkage between net operating income (profits) and IT investments is missing. This research further amplifies the complexity introduced by increased security requirements. However, one possible explanation for this lack of correlation between IT investments and profitability could be the absence of other organizational and environmental factors not included in the study (Sicar et al., 2000). For example, the high costs of IT project itself (whether outsourced or developed in house) could drain enormous amount of a firm's resources. Another possible explanation is that the wrong measurement methods (metrics) are being used for the complexity of value information available. Still, the major issue for many organizations involves trying to discover ways to effectively make IT/IS investments along with a sound security infrastructure that will result in productivity gains, competitiveness gains and other tangible and intangible benefits.

This is not a new problem nor will it ever disappear. While security infrastructure further increases IT overhead, historically, researchers attribute the shortfall in measuring IT value contribution to deficiencies in measurements and methods as well as to mismanagement of the technologies by developers and users of IT (Brynjolfsson, 1993). Weill (2003) suggests that a key issue to transform investments in IT into gains is the ability of a firm to transform its IT spending into economic value or social value. Past research has suggested information value approaches to

assess the contribution of IT in an organization (Ahituv, 1989). According to Ahituv (1989), an information value method consists of three framing concepts for assessing the value of information: normative, real, and perceived. Therefore, in the following paragraphs an explanatory analysis of the approaches available to estimate measures of information value (Normative, Real, and Perceived) will be conducted to determine both their positive and negative impacts on measuring the value contribution of IT and the required security infrastructure. An information value framework is presented to aid in understanding information value metrics.

Normative Value Approach:

The Normative Approach is used to predict what *should* be, based on observation, deduction, and generalization, often using models and computations. Essentially, this approach is used to develop some type of ranking mechanism, evaluating information results of various systems.

Methods and assumptions ranking these results are based on computational models such Bounded Rationality, Prospect Theory, and Utility Theory. A good example of an attempt to apply a normative model, in this case Utility Theory, as a ranking mechanism to determine the value of a system was Ahituv and Berman (1988). Their research used a rational decision normative model to evaluate information systems, in this case, the dispatching of emergency equipment. It was assumed that the objective of a dispatcher was to minimize the expected response time to a call. It was demonstrated computationally that a real-time IS can improve the performance of a network better than information delayed types of systems. In this case, the Normative Approach to information value attempts to justify an information system because of quantifiable productivity gains in comparison to other systems.

In this sense of application and framing, the Normative model may seem to be capable of answering the information value measurement for productivity gains. However, it seems incapable of measuring other information value issues such as regulatory requirements, competitive power, management skill, other real world issues. As stated in Ahituv (1989) Normative Approaches have the following weaknesses:

1. Difficult to model a real life information system because it requires formulations of all components on an information system (including human entities)
2. With the definition of mathematical relationships, it is still difficult to calibrate the model by introducing real figures.
3. Models may become so complex that they exceed our capacity to resolve them analytically.

In relation to information value, the Normative Approach has been shown to demonstrate the ability to rank systems in relation to their value. This approach can be particularly useful for IT security investments as it is hard to know how likely an organization will be exposed to a security loss and to quantify it. However, using a ranking Normative value approach as a justification tool, the ranking could be used to compare 'No system' options, thus potentially answering some of the justification qualms often explored by IT Managers and CSO's.

Real Value Approach:

The Real Approach is based upon measuring differences in performance, before and after examination. Empirical research methods are used to monitor and control implemented or prototyped systems to review their potential impacts (real-life cases and experiments). This approach is well-suited for examination of many information value issues.

Many studies have examined the before and after impacts of systems implementation. One particularly noteworthy example of this type of research was conducted by Eveland & Bikson (1988).This field experiment set out to show the interdependency of group structures and technology. To conduct the experiment, the project enrolled 79 male members, all of them prior professionals, distributed into two equal groups in two different environments, one with e-mail technology and the other without. The experiment found that the group without e-mail technology developed into a traditional hierarchical structure during project assignment. The group with computer technology formed a natural team environment where, with every new project assigned, new technical leaders emerged. As opposed to a single (constant) team leader as with the traditional hierarchy, the natural team shifted command to those people with technical knowledge in the specific area of each project assigned. Overall, the e-mail group projects were more thorough, innovative, and after the initial learning curve more timely.

This basic Real Approach example demonstrates that a particular IS system, in this case e-mail, created a transformation that increased productivity and quality. This Real Approach answers the productivity and environmental effects of IT investments in real-world situations.

The Real Approach is not without its weaknesses in applicability. According to Ahituv (1989), the Real measure has several problems for quantifying IS benefits:

1. Accuracy of measurement. The Real Approaches examine the outcomes generated rather than the actual workings and manipulations of the IS.
2. An implemented system must exist for measurement to take place

While these are serious drawbacks, the main drawback in relation to measuring information value is the fact that an implemented system must be in place. In order to justify building a new system, using the Real Approach of information value would require benchmarking similar organizations or building testable prototypes. This may be inherently difficult to measure for large projects such as an ERP implementation. Adding security to the mix, such as whether to use role based security over role-based with biometric technology is extremely difficult to measure benefits (Herrod, 2005). However, if the situation permits, as an after the fact measurement, or as a prototype evaluation tool, the Real Approach is a very good implement for defining the value of information systems and address concerns of valuing IT/IS and security investments. This may explain the ubiquity of Real Approaches such as ROI and ROA.

Perceived Value Approach:

The Perceived Approach is based on subjective evaluations performed by users of an information system. Similar to the Real Approach, empirical research methods are used to monitor and control implemented or prototyped systems to review their potential impacts (usually via some type of survey tool). This approach is well-suited for examination of information security value issues where risks are uncertain.
To illustrate how the Perceived value approach works, Ahituv (1989) discusses two main types of notable Perceived Approach studies, willingness to pay and semantic scales. In willingness to pay experiments, decision makers are asked how much they would be willing to pay for, maintain, and make accessible different type of information outputs from a system.

By using this 'willingness to pay' method by comparing a list of alternative systems (or features), one can assess the value and needs of the system. In an information security value sense, getting input regarding preferences and perceptions about system risks gives good input regarding the perceived value of the system from the people that actually use it and the decisions makers evaluating it.

In the semantic scale method, users are asked to rank systems and features on differential scales. By analyzing the rankings, one can assess the values users associate with the system. Information value, which is often perceptually based, can be framed within the perceptions of users as to how users rank the effectiveness of the system.

The Perceived Approach is not without its weaknesses in applicability. According to Ahituv (1989), the Perceived measure has several problems for quantifying information value:

1. Point of measurement. The Perceived Approaches examine the outcomes generated by the decision maker rather than the outcome generated by the system. While this does separate Real from Perceived, a user might believe a system to be good, whereas in a Real sense another system might be better (i.e. an insecure system may be easier to log into, therefore perceived superior to a more secure system).
2. Voluntary system. One must have subjects to survey who are qualified to make these judgments.

Despite its weaknesses, the Perceived Approach is an excellent tool for long range plans (based on perceptions of where the organization needs to be) and measuring intangible assets. The Perceived Approach is a very good implement for defining the value of information systems and addressing some of the long range benefits concerns of measuring information security value where hard metrics are difficult to obtain.

DISCUSSION

Taking each approach separately (Normative, Real and Perceived) one finds gaps in their application. However, perhaps the question is not choosing one approach to valuing IS/IT and security investments, but rather where and when to use to appropriate approach. Figure 1 bonds the traditional organization "Anthony's model" with the three measurement approaches, suggesting them as a guide of where one may use a Normative, Real, or Perceived Approach within an organization (Figure 1).

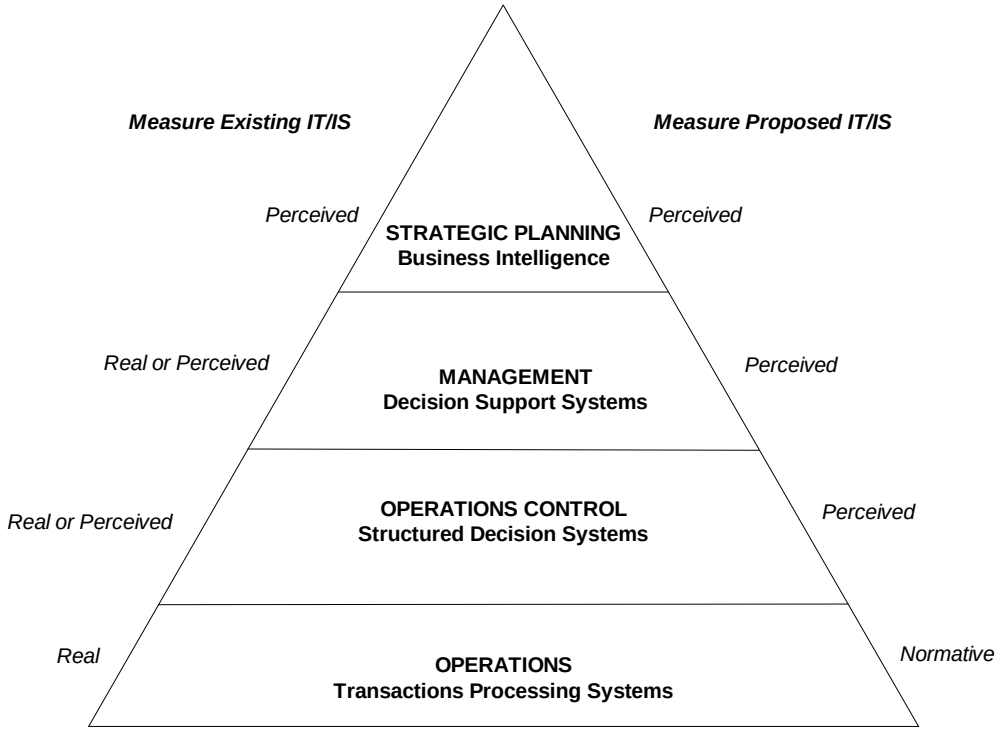

Figure 1: Application of Value Measurements (adapted from Ahituv 1989).

As Figure 1 shows, at the strategic level of an organization perceived value is a more appropriate choice as the complexity of the whole organization underneath makes it next to impossible to separate the information from the system (security, people, hardware, software, etc.) processing it. The scope from this strategic level is often too large. Likewise, on the bottom level of the diagram (operations), the scope of decision making is much more limited. Therefore it is easier to, due to a smaller number of variables, to analyze normative and real data. As Figure 1 also shows, measuring existing systems and security infrastructure merits different approaches than evaluating proposed solutions. Most notably, Real approaches are more suitable at the operations level to use for an existing IT/IS due to their reliance on 'before and after' analyses, rather than a proposed IT/IS evaluation where 'before' data may not exist. Overall, in terms of determining information value approaches, this model may go far in helping IS professionals justify the security investments within the systems they sponsored.

The measurement of information value involves differing perceptions of what should be the return on investment of an information system. The CIO, CSO, and the CEO often have differing view i.e. quality, improvements versus profits. To answer these concerns from an information management and security standpoint, we have examined three approaches for measuring the value of information systems (Normative, Real, Perceived). The result one may consider is that there is always some type of contribution, it just depends how you measure it. In order to evaluate the value of information systems and security investments to answer issues commonly raised by organizations, one may need to use *all* of the approaches described previously as they each contain their own strengths and weaknesses. Banker et al (1993) suggests the need for models and metrics with multiple evaluative perspectives, the need for longitudinal and permanent analysis (along the conversion processes), and that to increase the likelihood of success, measurements should be made as close to the locus of the value as is feasible. In essence, one may need to choose a variety of approaches depending on the situation as it exists.

REFERENCES

Applegate L., Austin R., Mcfarlan, W. (2003). *Corporate Information Strategy and Management (Text and Cases)*. New York: McGraw-Hill Irwin, 2003.

Ahituv, N. (1989). Assessing the value of information: Problems and approaches. *Proceeding of the 10th International Conference on Information Systems*, Boston, MA. December, 315-325.

Ahituv, N. & Berman, O. (1988). *Operations Management of Service Networks - A Practical Quantitative Approach*, Plenum Press, New York, 293 pages.

Banker, R. D., Kauffman, R. J, and Mahmood, M. A. (1993). Measuring the Business Value of IT: A future oriented perspective, In Khosrowpour,M and Mahmood, M. A. (Eds.) *Strategic Information Technology Management Series*.

Brynjolfsson, Erik (1993). The Productivity Paradox of IT. *Communications of the ACM*, 36:12, Dec.

David, P.A. (1989). Computer and Dynamo: The Modern Productivity Paradox In A Not-Too Distant Mirror. *The Warwick Economics Research Paper Series (TWERPS) 339*. Department of Economics, University of Warwick.

Eveland, J. D., & Bikson, T. K. (1988). Work group structures and computer support. *ACM Transactions on Office Information Systems*, 6(4), 354-379.

Herrod, C. (2006, in press). The role of Information Security and its Relationship to Information Technology Risk Management, In Whitman and Mattord (Eds.) *Readings and Cases in the Management of Information Security*, Thomson, pp45-61.

Lee, J. and Bose, U. (2002). Information Technology Investments and Multifaceted Aspects of a Firm's Economic Performance. *Journal of Information Technology*, (17:3), Sep. , p119.

Mitra, S. and Chaya, A. (1996) Analyzing Cost-Effectiveness of Organizations: the Impact of Information Technology Spending. *Journal of Management Information Systems*, (13:2), p29-57.

Mahmood, M.A. and Mann, G.J. (1993) Measuring the Organizational Impact of Information Technology Investment: An Exploratory Study. *Journal of Management information System*, (10:1), p 97-122.

Nicolett, M. (2004). IT Security challenges can address regulatory compliance. *Gartner Research Note COM-22-1253*. Boston: Gartner Group Publishing.

Sircar, S., Turnbow, J.L and Bordoloi, B. (2000). A framework for Assessing the Relationship Between Information Technology Investments and Firm Performance. *Journal of Management Information Systems*, (16:4), p69-97.

Weill, Peter. (2003). The relationship between investment in information technology and firm performance: a study of the valve manufacturing sector. *Working papers no. 239*, Massachusetts Institute of Technology (MIT), Sloan School of Management.